DETEKSI POSISI PESAN RAHASIA PADA STEGANOGRAFI CITRA BERBASIS ANALISIS RAW QUICK PAIR(RQP) DAN DISCRETE WAVELET TRANSFORM(DWT)

SECRET MESSAGE POSITION DETECTION IN IMAGE STEGANOGRAPHY BASED ON RQP ANALYSIS AND DISCRETE WAVELET TRANSFORM(DWT)

Apriza A W[1], Iwan Iwut Tritoasmoro,S.T.,M.T.[2], I Nyoman Apraz Ramatryana, S.T., M.T.[3]
[1,2,3]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
Jln. Telekomunikasi No.1 Terusan Buah Batu Bandung 40257 Indonesia
1 **aprizaaw@student.telkomuniversity.ac.id** , 2**iwan.tritoasmoro@gmail.com** ,
3ramatryana@telkomuniversity.ac.id

Abstrak

Steganografi citra adalah proses penyisipan pesan rahasia atau pesan stego pada citra digital namun tidak terlihat atau tidak diketahui oleh penglihatan mata manusia. pesan stego yang susah diketahui tersebut menyebabkan perlunya suatu teknik untuk mengetahui keberadaan sebuah pesan steganografi di sebuah citra digital yang dinamakan steganalisis.

Penelitian ini melakukan analisis sistem Steganalisis citra berdasarkan fitur *discrete wavelet transform* (DWT) dan analisis *raw q uick pair* (RQP). Hasil dari DWT adalah subband yang terpisah secara frekuensi. Selanjutnya subband tersebut dihitung untuk mendapatkan nilai RQP. Nilai RQP digunakan untuk klasifikasi KNN. Pada penelitian ini, hasil klasifikasi KNN adalah kelas citra asli dan kelas citra stego. Parameter performansi dari penelitian ini adalah akurasi dan waktu komputasi.

Kata Kunci: ***Steganalysis*, RQP *Raw Quick Pairs*, DWT *Discreate Wavelet Transform*, KNN *K-Nearest Neighbor*.**

Abstract

Image steganography is the process of inserting a secret message or stego message on a digital image but not visible or unknown to the human eye. the unknown stego message caused the need for a technique to find out the existence of a steganographic message in a digital image called steganalysis.

This research analyzes the image steganalysis system based on discrete wavelet transform (DWT) and raw quick pair (RQP) analysis. The result of DWT is a subband that is frequency separated. Furthermore, the subband is calculated to get the RQP value. The RQP value is used for the KNN classification. In this study, the classification of KNN is the original image class and the stego image class. The performance parameters of this study are accuracy and computational time.

Keywords: Steganalysis, raw quick pair, discrete wavelet transform, DWT, RQP

1. Pendahuluan

1.1 Latar Belakang

Seiring dengan perkembangan era globalisasi semakin meningkat pula kebutuhan akan teknologi informasi. Semakin banyak tuntutan atau permintaan akan kebutuhan teknologi mengakibatkan menipisnya ruang privacy seseorang. Oleh karena itu, terciptalah steganografi yang merupakan teknik atau cara penyisipan suatu pesan rahasia kedalam teks, gambar untuk menyembunyikan kode atau pesan rahasia dari orang tertentu

Pada penelitian sebelumnya telah dilakukan pengembangan *steganalysis* dengan metode *Binary Similarity Measures – Support Vector Machine* (BSM-SVM) dengan tujuan pengujian apakah metode ini bisa mendeteksi teknik *steganography* LSB dan F5 pada format BMP dan JPG. Berdasarkan pengujian yang telah dilakukan terhadap citra digital, algoritma BSM-SVM mampu mendeteksi metode LSB dan F5 dan memiliki nilai akurasi yang mencapai 77,28% untuk deteksi metode LSB dan 76,49% untuk deteksi metode F5. Metode ini juga mampu diterapkan pada format citra digital berupa JPG dan BMP dimana pada JPG akurasinya mencapai 77,02% dan pada BMP sebesar 76,75%[1]. Steganalysis dengan metode uji *ChiSquare* dalam domain *Discrete Wavelet Transform* (DWT) memiliki nilai akurasi sebesar 52,57% untuk citra dengan ukuran baris 256 dan 58,37% untuk citra dengan ukuran baris 512. Dimana penggunaan DWT jenis db4

memberikan nilai akurasi yang lebih baik yaitu 61,77% dibandingkan dengan DWT jenis haar nilai akurasinya hanya 49,14% dan perbedaan jumlah level yang digunakan pada transformasi mempengaruhi akurasi pendeteksian[2]. Tugas akhir (TA) ini akan melakukan studi dan analisis pada sistem Steganalisis pada citra *digital* berdasarkan fitur yang berasal dari citra hasil steganografi di domain transformasi *discrete wavelet transform* (DWT) dan analisis *raw quick pair* (RQP). Citra digital ditransformasi DWT untuk mendapatkan *subband* yang terpisah sesuai dari frekuensi.

Parameter keberhasilan simulasi ini adalah akurasi (ACC), rasio deteksi atau *detection rate* (DR), dan *false positive rate* (FPR). Hipotesis terhadap simulasi teknik steganalisis menggunakan metode DWT dan RQP adalah memiliki ACC yang baik yaitu minimal 78%, DR lebih dari 50%, dan FPR lebih kecil dari 30%.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, maka rumusan masalah dari TA ini adalah sebagai berikut:

1. Bagaimana perancangan steganalysis pada domain DWT dan RQP.
2. Bagaimana pengaruh paramater ukuran gambar, ukuran pesan, level DWT, dan paramter RQP terhadap akurasi steganalysis.
3. Bagaimana performansi sistem yang sudah dirancang.

1.3 Tujuan Masalah

Berdasarkan latar belakang tersebut, maka rumusan masalah dari tugas akhir ini adalah sebagai berikut:

1. Merancangan steganalysis pada domain DWT dan menggunakan metode RQP
2. Menganalisis pengaruh paramater ukuran gambar, ukuran pesan, level DWT, dan paramter RQP terhadap akurasi steganalysis
3. Menganalisis performansi sistem yang sudah dirancang

1.4 Batasan Masalah

Agar permasalahan yang dibahas terfokus dan tidak melebar, tugas akhir ini memiliki batasan-batasan masalah sebagai berikut :

1. Citra digital yang digunakan berformat citra .bmp dengan resolusi 128×128, 256×256, dan 512×512.
2. Citra yang digunakan citra RGB.
3. Parameter performansi yang diteliti dan dianalisis yaitu Akurasi
4. Proses stegano dengan menggunakan metode LSB dan tidak membahas teknik steganography
5. Steganalisis yang digunakan bersifat pasif yang hanya dapat mendeteksi keberadaan pesan dan posisi pesan yang terdiri dari posisi awal, tengah, dan akhir.

1.5 Metode Penelitian

Metode yang dilakukan untuk menyelesaikan tugas akhir ini adalah sebagai berikut :

1. Studi Literatur

Mempelajari referensi yang mendukung dalam perancangan serta pengerjaan tugas akhir ini. Literatur yang dijadikan sumber berasal dari buku, jurnal ilmiah dan referensi lain yang berkaitan.

2. Perancangan dan Analisis

Melakukan perancangan program dengan menggunakan software MATLAB 2017b dan menganalisis hasil yang dihasilkan oleh perancangan.

3. Implementasi

Melakukan simulasi terhadap hasil perancangan dan analisis dengan membuat codingan di software MATLAB 2017b.

1.6 Sistematika Penulisan

Sistematika penulisan laporan adalah sebagai berikut:

Bab 1 PENDAHULUAN

Bab ini berisi latar belakang, permasalahan, tujuan, metode penelitian, serta sistematika penulisan pada tugas akhir yang dibuat.

Bab 2 DASAR TEORI

Bab ini akan menguraikan dasar teori yang berhubungan dengan permasalahan yang akan dibahas seperti latar belakang adanya steganalysis dan penjelasan metode-metode yang biasa digunakan dalam perancangan steganalysis.

Bab 3 SISTEM MODEL

Bab ini akan membahas pemodelan sistem berupa diagram alir yang akan dilakukan untuk melakukan analisis terhadap pengujian serta spesifikasi dari perangkat yang digunakan.

Bab 4 SIMULASI DAN ANALISIS

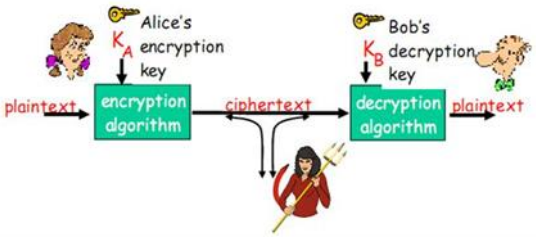
Bab ini akan menjelaskan tentang pengujian implementasi penggunaan metode DWT dan RQP serta menganalisis menggunakan Software MATLAB.

Bab 5 KESIMPULAN DAN SARAN

Bab ini akan berisi kesimpulan dan saran yang dapat dilakukan untuk penelitian selanjutnya dari pengerjaan tugas akhir.

2. Dasar Teori

Steganography yang merupakan teknik atau cara penyisipan suatu pesan rahasia kedalam teks, gambar maupun video untuk menyembunyikan kode atau pesan rahasia dari orang tertentu. Steganography berasal dari bahasa Yunani dimana ”steganos” berarti tersembunyi atau rahasia dan ”graphy” yang berarti menulis atau menggambar maka arti secara harfiah berarti menulis tersembunyi. Steganography menggunakan teknik untuk menyampaikan informasi dengan cara yang tersembunyi steganalysis.



Gambar 1. Framework of Steganography

2.1 *Steganalysis*

Steganalysis merupakan suatu teknik atau cara untuk mematahkan steganography dimana untuk mengetahui suatu media tersisipi pesan rahasia atau tidak. Untuk mengetahui ada atau tidaknya pesan rahasia di suatu media steganalysis mengumpulkan beberapa data untuk diamati dan untuk membedakan apakah carrier sebagai ‘stego’ atau ‘cover’ [4]. Citra sangat sering digunakan dalam steganalysis sebagai pembawa karena jumlah nya yang banyak dan memiliki resolusi piksel yang tinggi. Terdapat dua klasifikasi pada steganalysis, diantaranya:

1. **Specific Steganalysis**
   merupakan pendekatan secara spesifik yang menggambarkan kelas pada teknik steganalysis citra yang bergantung pada algoritma yang digunakan serta memiliki tingkat keberhasilan yang tinggi untuk mendeteksi ada atau tidaknya pesan rahasia
2. **Generic Steganalysis**
   atau biasa disebut dengan blind steganalysis yang dapat bekerja pada algoritma steganography yang diketahui maupun tidak tetapi memiliki akurasi yang kurang akurat dibandingkan spesific steganalysis.

2.2 Citra Digital

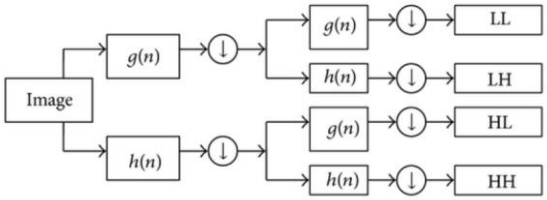
Citra digital dapat didefinisikan sebagai fungsi dua variabel, f (x;y), dimana x dan y adalah koordinat spasial dan nilai f (x;y) adalah intensitas citra pada koordinat tersebut [5]. Pengolahan citra digital merupakan teknik atau tata cara mengolah citra. Terdapat beberapa aplikasi dalam pengolahan citra digital, diantaranya *color image*, *grayscale image*, dan *binary image*.

2.3 *Discrete Wavelet Transform* (DWT)

Transformasi wavelet adalah sebuah transformasi matematika yang digunakan untuk menganalisis sinyal bergerak. Sinyal bergerak ini dianalisis untuk didapatkan informasi spektrum frekuensi dan waktunya secara bersamaan. Salah satu seri pengembangan transformasi wavelet adalah Discrete Wavelet Transform (DWT) [6].

Discrete Wavelet Transform DWT merupakan salah satu kakas yang banyak digunakan dalam teknik blind watermarking dan escrow watermarking dengan domain transform. Watermarking yang berbasis wavelet adalah pendekatan yang populer karena kekuatannya melawan malicious attack. DWT membagi sebuah dimensi sinyal menjadi dua bagian,

biasanya bagian dengan frekuensi tinggi dan frekuensi rendah,yang disebut dengan dekomposisi[7].



Gambar 2. Proses Dekomposisi Wavelet

2.4 Least Significant Bit (LSB)

LSB (Least Significant Bit) Coding. Metoda ini merupakan metoda yang sederhana. Metoda ini akan mengubah nilai LSB (Least Significant Bit) komponen luminansi atau warna menjadi bit yang bersesuai dengan bit label yang akan disembunyikan. Memang metoda ini akan menghasilkan video rekontruksi yang sangat mirip dengan aslinya, karena hanya mengubah nilai bit terakhir dari data. Metoda ini paling mudah diserang, karena bila orang lain tahu maka tinggal membalikkan nilai dari LSB-nya maka data label akan hilang seluruhnya[8].

2.5 Raw Quick Pairs (RQP)

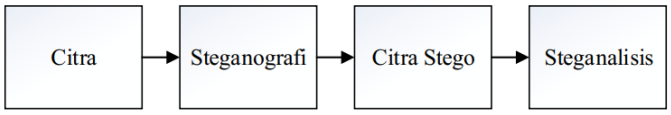
RQP meupakan metode steganalisis untuk mendeteksi penyisipan Least Significant Bit (LSB) pada citra berwarna 24-bit yang telah diusulkan oleh Fridrich. Metode ini melakukan analisis pasangan kemiripan warna yang disebabkan oleh penyisipan LSB. Rasio kemiripan warna dan jumlah warna unik yang meningkat secara signifikan saat pesan panjang yang dipilih disematkan di gambar sampul dan bukan pada gambar stego. Perbedaan inilah yang memungkinkan untuk membedakan antara gambar sampul dan gambar stego untuk kasus steganografi LSB. Metode ini bekerja dengan andal baik selama jumlah warna unik pada gambar sampul kurang dari 30 persen jumlah piksel. Seperti yang dilaporkan metode ini memiliki tingkat deteksi yang lebih tinggi daripada metode yang diberikan oleh Westfeld dan Pfitzmann namun tidak dapat diterapkan pada grayscale. Raw Quick Pairs memiliki fokus utama untuk mendapatkan satu atau lebih colordepth tinggi gambar digital untuk artefak statistik yang disebabkan oleh data tersemat menggunakan metode Least Significant Bit (LSB)[9].

2.6 K-Nearest Neighbor (K-NN)

K-NN merupakah salah satu metode klasifikasi pada citra yang berdasarkan ciriciri data pembelajaran (data latih) yang paling mendekati objek. Dimana ciri direpresentasikan dengan ukuruan jarak yang akan diolah dalam hitungan matematis. Dalam metode K-NN akan dihitung nilai jarak antara titik yang merepresentasikan data pengujian dengan semua titik yang merepresentasikan data latihnya.

3. Sistem Model

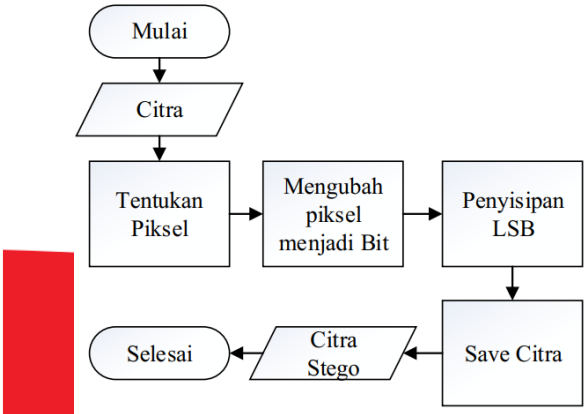
Sistem pada tugas akhir ini dibagi menjadi empat blok sistem, yaitu citra digital, steganografi, citra stego, dan steganalisis. Citra sebanyak 20 dipisah menjadi 10 citra latih dan 20 citra uji. Citra Latih dan citra uji selanjutnya disisipkan pesan pada proses steganografi menggunakan metode LSB. Hasil dari proses steganografi adalah citra stego yang disisipkan pesan rahasia dengan jumlah karakter yang berdeda dan posisi yang berbeda. Proses steganalisis menggunakan klasifikasi K-NN dengan ciri dari hasil DWT dan RQP. Klasifikasi K-NN terdiri dari dua tahap, yaitu tahap pelatihan dan tahap pengujian. Tahap pelatihan sebagai pencarian nilai parameter terbaik yang menjadi acuan sebagai database untuk klasifikasi K-NN dan tahap pengujian sebagai proses yang digunakan dalam tahap pengujian data.



Gambar 3. Diagram Blok Perancangan Sistem

3.1 Steganografi

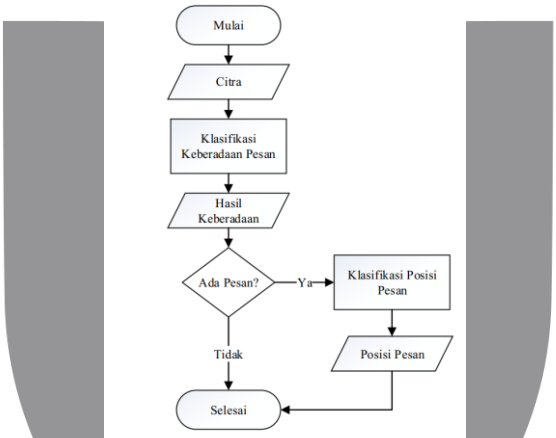
Proses steganografi bertujuan untuk membuat data citra stego yang sudah tersisipi pesan rahasia. Metode penyisipan menggunakan metode LSB. Gambar 4 menunjukkan proses steganografi.



Gambar 4. Diagram Alir Steganografi

3.2 Steganalisis

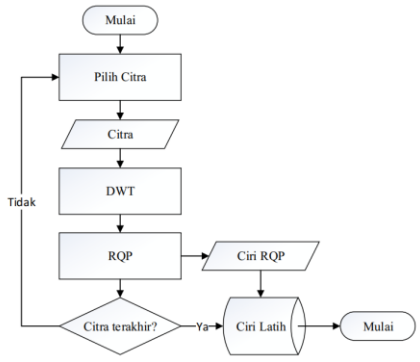
Proses model steganalisis merupakan suatu tahapan analisis ada atau tidaknya ´ pesan suatu data stego pada file host citra. Pada Gambar 5 menunjukan proses penyisipan dari perancangan sistem.



Gambar 5. Diagram Alir Steganalisis

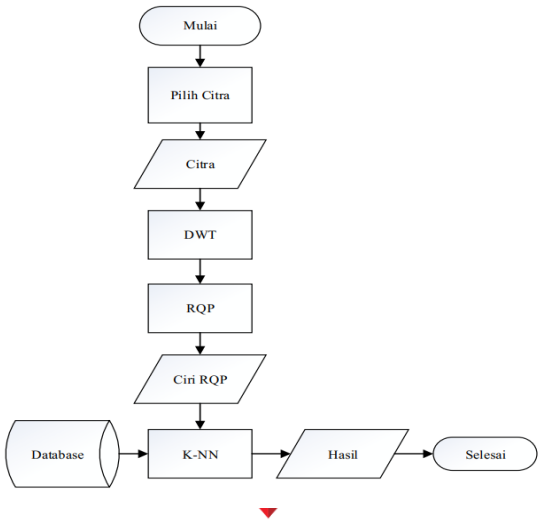
3.2.1 Proses Pelatihan

Proses ini merupakan proses pengambilan data latih dari suatu stego citra yang akan dimasukkan kedalam database.



Gambar 6. Diagram Alir Pelatihan Klasifikasi

3.2.2 Proses Pengujian

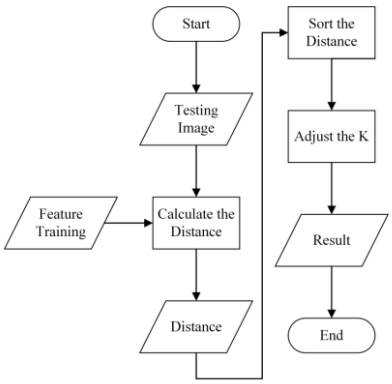


Gambar 7. Blok Alir Pengujian Klasifikasi

Berikut langkah-langkah dari pengujian steganalisis adalah sebagai berikut:

1. Pemilihan citra uji yang digunakan sebagai pendeteksi steganografi
2. Melakukan proses transformasi DWT pada citra uji.
3. Hasil citra yang sudah di transformasikan akan di hitung RQP untuk mendapatkan ciri masing-masing kelas yang digunakan untuk membedakan masingmasing kelas
4. Setelah didapatkan ciri pada citra uji akan dilakukan proses klasifikasi menggunakan K-NN yang berdasarkan data dalam database. Hasil klasifikasi K-NN akan disimpulkan apakah citra uji teridentifikasi sebagai citra asli atau citra yang tersisipi.

3.2.3 Klasifikasi K-NN



Gambar 8. Diagram Alir Klasifikasi K-NN

Berikut langkah-langkah dari pengujian steganalisis adalah sebagai berikut:

1. Pemilihan citra uji yang akan di uji untuk proses steganalisis
2. Penentuan jumlah K tetangga sebagai data latihnya
3. Melakukan perhitungan jarak data latih dengan data ujinya menggunakan parameter Euclidean
4. Melakukan pengukuran jarak sesuai kelasnya
5. Pengambilan nilai jarak terkecil berdasarkan jumlah K tetangga dan kelas mayoritas

3.3 Performansi Sistem

Pengujian ini dilakukan untuk mengetahui performansi sistem sehingga dapat diketahui kekurangan dan kelebihan sistem. Performansi sistem diukur berdasarkan pada parameter-parameter berikut:

3.1 Akurasi Sistem

Akurasi suatu ukuran ketepatan sistem dalam mengenali masukan yang akan diberikan sehingga menghasilkan keluaran yang benar. Secara sistematis dapat ditulis sebagai berikut:

$$\text{Akurasi} = \frac{\text{Jumlah data benar}}{\text{Jumlah data keseluruhan}} \times 100\% \qquad (3.1)$$

3.2 Waktu Komputas

Waktu komputasi merupakan waktu yang diperlukan sistem untuk mengolah data sampai didapatkan keluaran yang diinginkan.

Waktu komputasi = Waktu akhir−waktu awal (3.2)

4. Pengujian dan Analisi

Pada bab ini, melaporkan pengujian dan analisis sistem untuk menguji performansi dari sistem steganalisis yang telah dirancang pada bab III. Pengujian terdiri dari 6 skenario yang terdiri dari:

1. Pengujian ukuran gambar terhadap akurasi deteksi keberadaan pesan dan deteksi posisi pesan.
2. Pengujian jenis subband DWT terhadap akurasi deteksi keberadaan pesan dan deteksi posisi pesan.
3. Pengujian level DWT terhadap akurasi deteksi keberadaan pesan dan deteksi posisi pesan.
4. Pengujian Mother DWT terhadap akurasi deteksi keberadaan pesan dan deteksi posisi pesan.
5. Pengujian nilai k dari K-NN terhadap akurasi deteksi keberadaan pesan dan deteksi posisi pesan.
6. Pengujian jenis jarak dari K-NN terhadap akurasi deteksi keberadaan pesan dan deteksi posisi pesan.

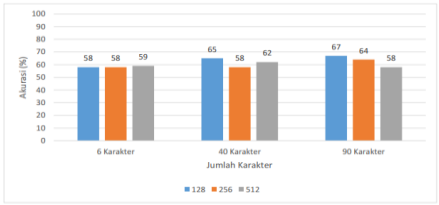
Tujuan pengujian adalah untuk mengetahui seberapa akurat kualitas system steganalisis citra terhadap penentuan ada atau tidak adanya pesan dan posisi pesan.

Pengujian sistem dalam penelitian ini dilakukan pada host citra yang berformat .bmp dengan sisipan berupa teks. Yang terdiri dari 3 ukuran pesan rahasia.

4.1 Pengujian Pengaruh Ukuran Gambar

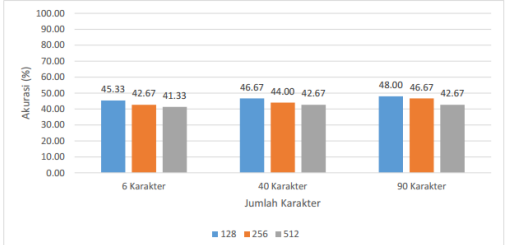
Pengujian pengaruh ukuran gambar bertujuan untuk mencari ukuran gambar yang memiliki hasil akurasi terbaik. Ukuran gambar yang diujikan adalah 128 × 128, 256 × 256, dan 512 × 512.

4.1.1 Pengujian Pengaruh Ukuran Gambar Terhadap Akurasi Keberadaan Pesan



Gambar 9. Akurasi Keberadaan Pesan Pengujian Ukuran Gambar

4.1.2 Akurasi Posisi Pesan Pengujian Ukuran Gambar

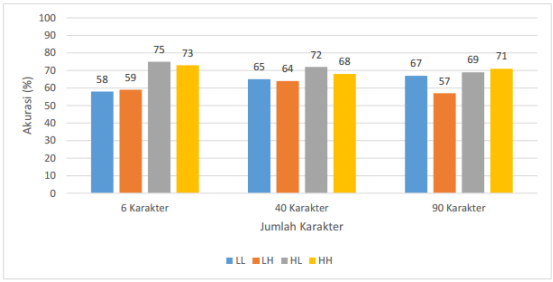


Gambar 10. Akurasi Posisi Pesan Pengujian Ukuran Gambar

4.2 Pengujian Pengaruh Subband DWT

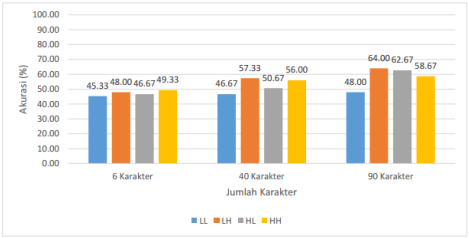
Pengujian subband DWT bertujuan menguji jenis subband DWT terhadapakurasi deteksi keberadaan pesan dan deteksi posisi pesan. Langkah pengujian dan banyaknya data latih.

4.2.1 Pengujian Pengaruh Subband DWT Terhadap Akurasi Keberadaan Pesan



Gambar 11. Akurasi Keberadaan Pesan Pengujian Ukuran *Frame*

4.2.2 Pengujian Pengaruh Subband DWT Terhadap Akurasi Posisi Pesan

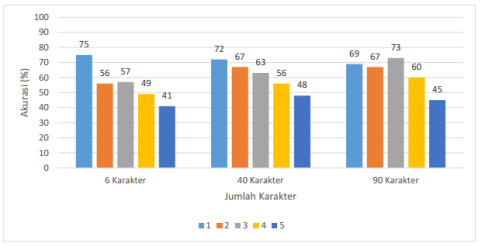


Gambar 12. Akurasi Posisi Pesan Pengujian Ukuran *Frame*

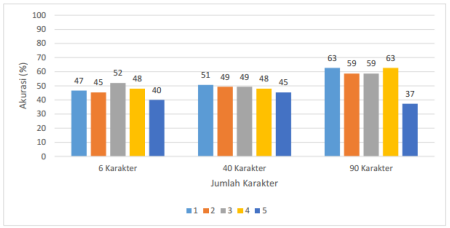
4.3 Pengujian Pengaruh Level pada DWT

4.3.1 Pengujian Pengaruh Level DWT Terhadap Akurasi Keberadaan Pesan (A)

4.3.2 Pengujian Pengaruh Level DWT Terhadap (B)



Gambar (A)



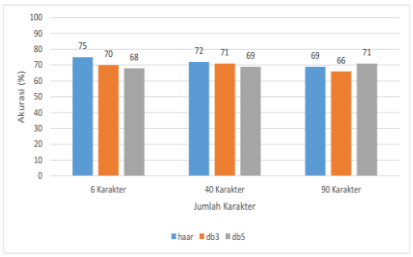
Gambar (B)

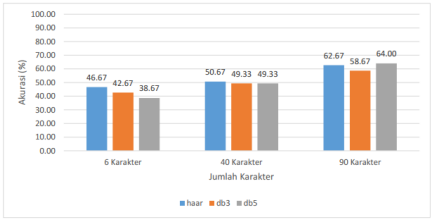
4.4 Pengujian Pengaruh Mother pada DWT

Pengujian ini mengubah jenis mother wavelet untuk menguji pengaruh mother wavelet pada DWT. Hasil pengujian mother wavelet juga menghasilkan akurasi yang tidak berubah seperti pengujian level DWT.

4.4.1 Pengujian Pengaruh Mother DWT Terhadap Akurasi Keberadaan Pesan (A)

4.4.2 Pengujian Pengaruh Mother DWT Terhadap Akurasi Posisi Pesan (B)





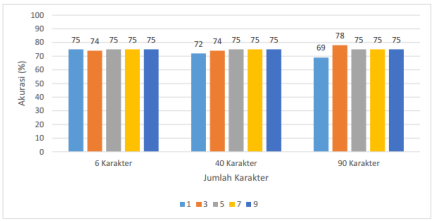
Gambar (A) **Gambar (B)**

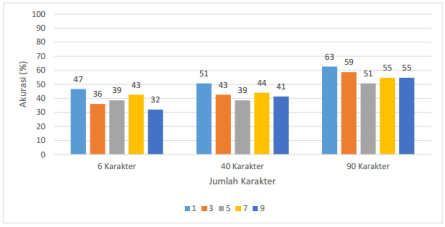
4.5 Pengujian Pengaruh K pada Klasifikasi K-NN

Nilai K merupakan nilai yang mengatur banyaknya ketetanggaan pada K-NN, semakin besar nilai k maka jumlah tetangga yang digunakan untuk voting pengambilan keputusan dari klasifikasi K-NN semakin banyak.

4.5.1 Pengujian Pengaruh Nilai K Terhadap Akurasi Keberadaan Pesan (A)

4.5.2 Pengujian Pengaruh Nilai K Terhadap Akurasi Posisi Pesan (B)





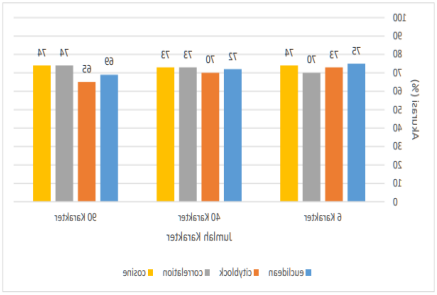
Gambar (A) **Gambar (B)**

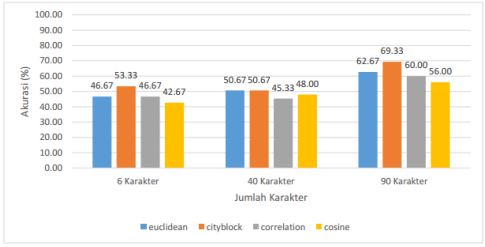
4.6 Pengujian Pengaruh Jarak K-NN

Pengujian ini bertujuan untuk mendapatkan parameter terbaik dari jenis jarak K-NN. Hasil dari pengujian keberadaan pesan menunjukkan hasil yang sama saat jenis jarak diubah.

4.6.1 Pengujian Pengaruh Jarak K-NN Terhadap Akurasi Keberadaan Pesan (A)

4.6.2 Pengujian Pengaruh Jarak K-NN Terhadap Akurasi Posisi Pesan (B)





Gambar (A) **Gambar (B)**

5. Kesimpulan dan Saran

5.1 Kesimpulan

Dari hasil pengujian yang dilakukan pada tugas akhir ini, dapat disimpulkan sebagai berikut.

1. Sistem yang dibuat mampu mendeteksi keberadaan pesan rahasia dan posisi pesan yang disisipkan menggunakan metode LSB.
2. Parameter akurasi terbaik untuk deteksi keberadaan pesan adalah ukuran gambar yang terbaik adalah 128×128. Parameter DWT terbaik adalah jenis subband HL, level sebesar 1, dan mother wavelet jenis haar. Parameter KNN yang terbaik adalah K dengan besar 1 dan jenis jarak euclidean. Akurasi terbaik sebesar 75%.

3. Parameter akurasi terbaik untuk deteksi posisi pesan adalah ukuran gambar yang terbaik adalah 128×128. Parameter DWT terbaik adalah jenis subband HL, level sebesar 1, dan mother wavelet jenis haar. Parameter KNN yang terbaik adalah K dengan besar 1 dan jenis jarak cityblock. Akurasi terbaik sebesar 69.33%.

5.2 Saran

1. Menambahkan metode untuk posisi deteksi dan volume, karena metode RQP tidak bisa untuk mendeteksi posisi dan volume.
2. Menambahkan jumlah data dan teknik penyisipan yang lain.
3. untuk penambahan deteksi posisi dan pesan kita harus mengetahui posisi dan volumea pesan saat melakukan steganografi.Menambahkan metode untuk posisi deteksi dan volume, karena metode RQP tidak bisa untuk mendeteksi posisi dan volume.

DAFTAR REFERENSI

[1] A. S. Nugraha, Impelementasi Steganalisis Dengan Menggunakan Metode BSM-SVM Pada Steganografi Citra Digital. Jurusan Teknik Informatika Universitas Telkom, 2013.

[2] A. Tantu, Steganalisis Dengan Metode Uji Chi-Square dalam Domain DWT. Jurusan Teknik Telekomunikasi Universitas Telkom, 2014.

[3] P. Richer, Detecting hiding information with computer forensic analysis. United States : SANS Institute, 2003.

[4] R. Chhikara and L. Singh, A Review on Digital Image Steganalysis Techniques Categorised by Features Extracted. India : ITM University, 2013.

[5] R. C. Gonzalez and R. E. Woods, Digital Image Processing, 2nd ed. Prentice Hall, Januari, 2002.

[6] P. Morettin, “Waves and wavelets: From fourier to wavelet analysis of time series,” Sao Paulo, Brazil: Institute of Mathematics and Statistics of University ˜ of Sao Paulo, 2004. ˜

[7] C. R. Mohamad Sulthon Fitriansyah, “Digital watermarking pada citra digital fotografi metode discrete wavelet transform,” JL.Soekarno-Hatta No. 9 Malang, 2015.

[8] C. Chan and L.M.Cheng, “Hiding data in images by simple lsb substitution,” March 2004.

[9] W. Shuozhong, Z. Xinpeng, and Z. Kaiwen, “Steganographic technique capable of withstanding rqp analysis1,” in Journal Of Shanghai University, vol. 06, no. 4, Sep. 2002.

[10] M. Fridrich, J. Goljan and R. Du, “Detecting lsb steganography in color and gray-scale images,” 2001.

[11] M. Fridrich, J. Long and R. Du, “Steganalysis of lsb encoding in color images,” 2000.

[12] A. Sukma, D. Ramadhan, Santoso, B. Puji, Sari, A. K. W. Tiara Ratna, and N. Made, “Tugas akhir k-nearest neighbor information retieval,” Surbaya: Jurusan Sistem Informasi Universitas Airlangga, 2014.

[13] Fadhillah, N. Armanda, M. Ledya Novamizanti, Ssi., Atmaja, and M. Ratri Dwi, ST., “Jurnal analisis dan implementasi klasifikasi k-nearest neighbor (k-nn) pada sistem identifikasi biometrik telapak kaki manusia,” Bandung: Jurusan Teknik Telekomunikasi Telkom University, 2015.